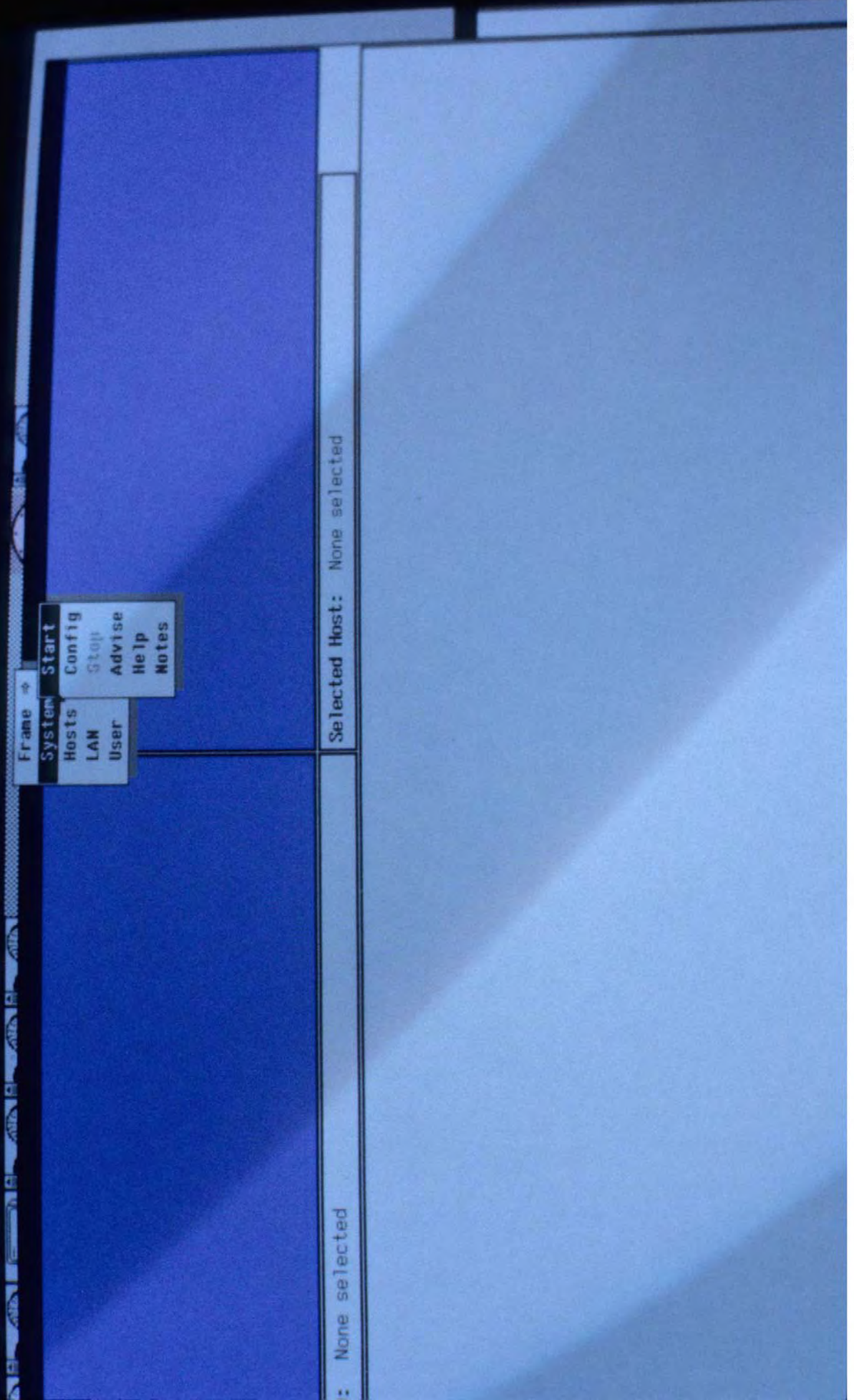


HEB\_0004923





HEB\_0004924



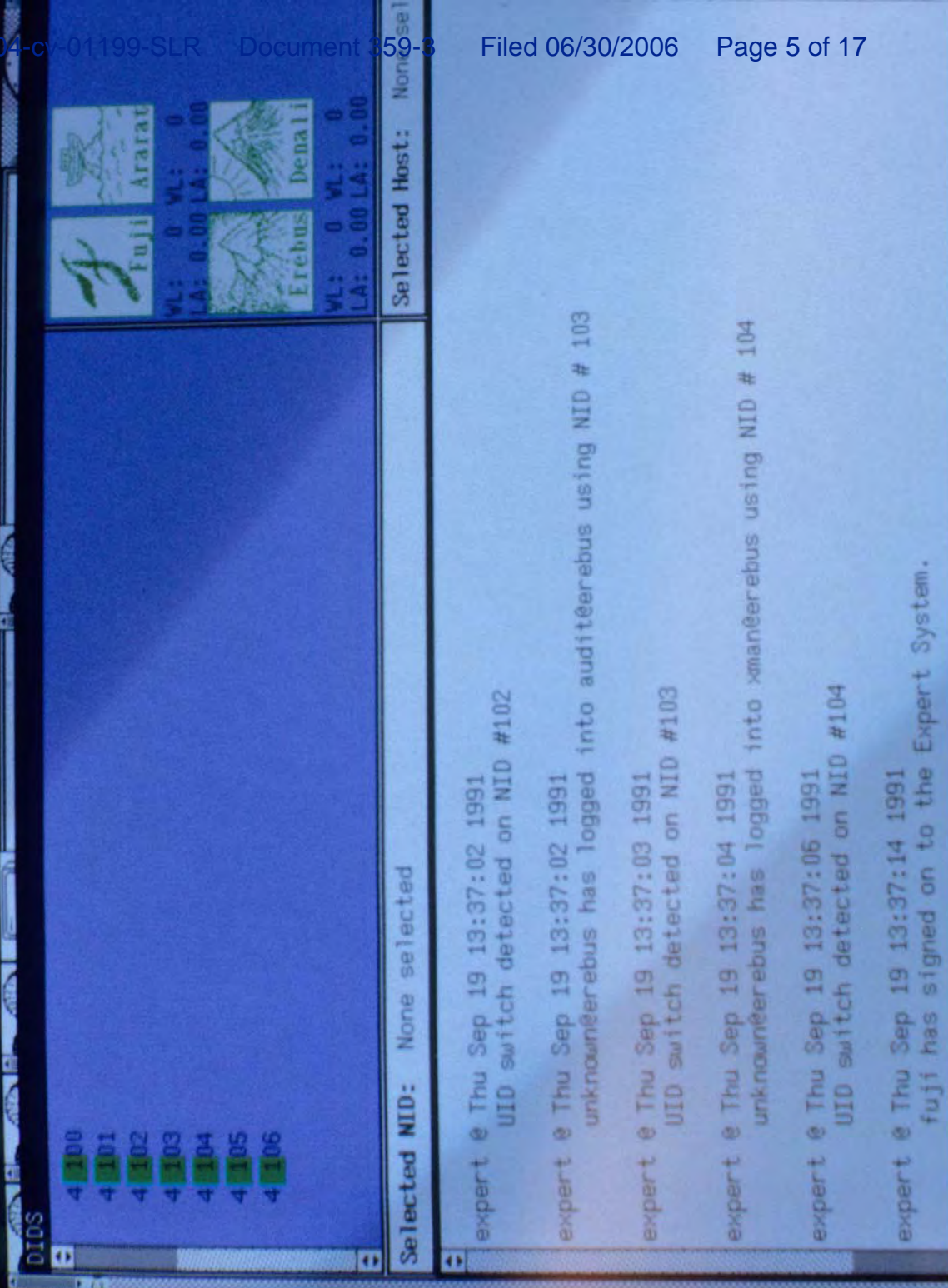


HEB\_0004925

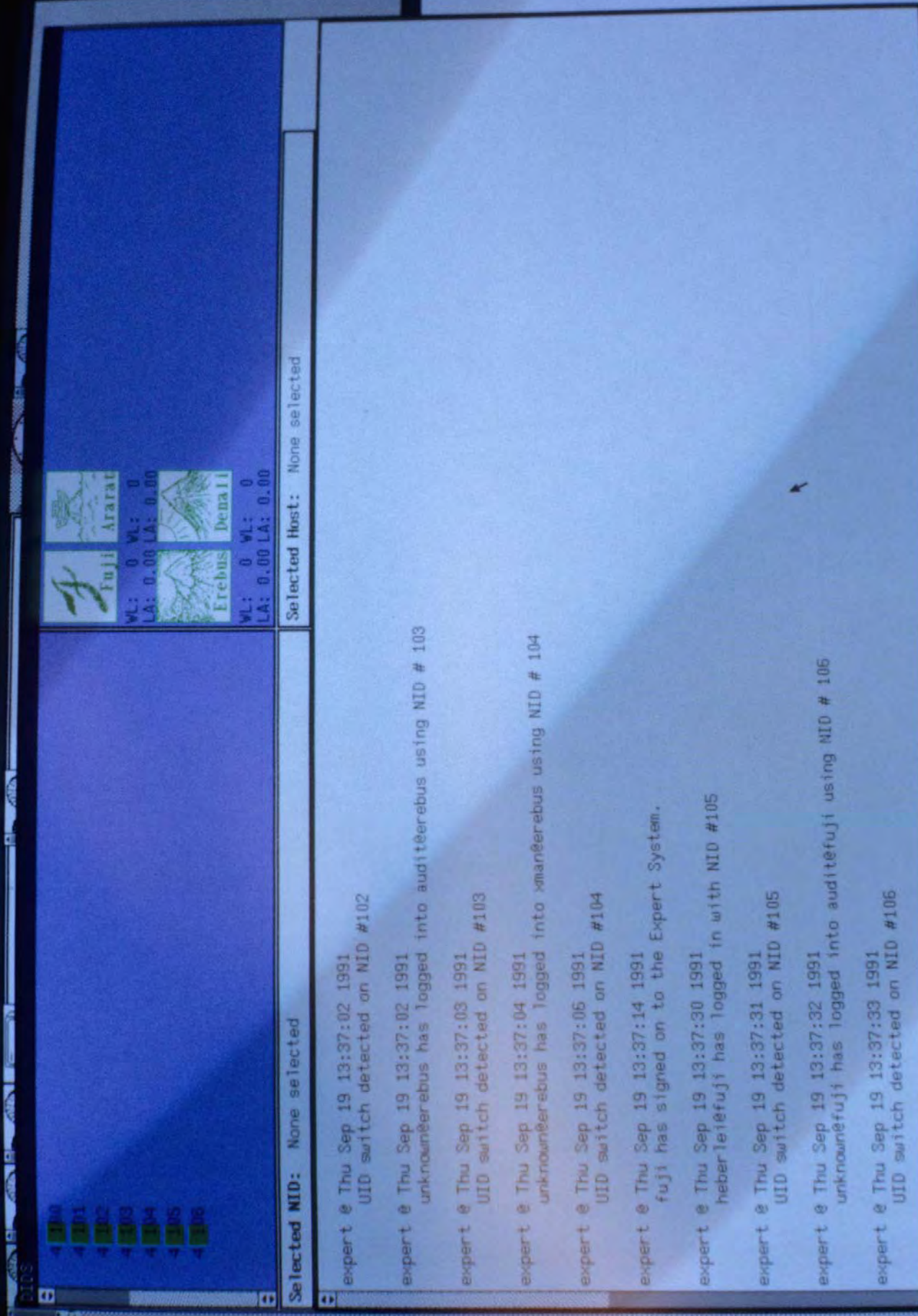
0 -1		DIDS	
			
Selected MID: None selected		Selected Host: None selected	

HEB\_0004926





HEB\_0004927



HEB\_0004928





VL: 0 VL: 0  
LA: 0.00 LA: 0.00

Selected Host: None selected

Selected NID: None selected

expert @ Thu Sep 19 13:37:30 1991  
heberle@fuji has logged in with NID #105

expert @ Thu Sep 19 13:37:31 1991  
UID switch detected on NID #105

expert @ Thu Sep 19 13:37:32 1991  
unknown@fuji has logged into audite@fuji using NID # 105

expert @ Thu Sep 19 13:37:33 1991  
UID switch detected on NID #106

expert @ Thu Sep 19 13:41:46 1991  
unknown@kongur has logged into dragyn@ararat using connection #2 and NID #107

expert @ Thu Sep 19 13:41:47 1991  
UID switch detected on NID #107

expert @ Thu Sep 19 13:41:49 1991  
Last login: String Match on connection #2

expert @ Thu Sep 19 13:41:51 1991  
Successful Tagged File access: /etc/passwd by unknown@kongur operating as dragyn@ararat

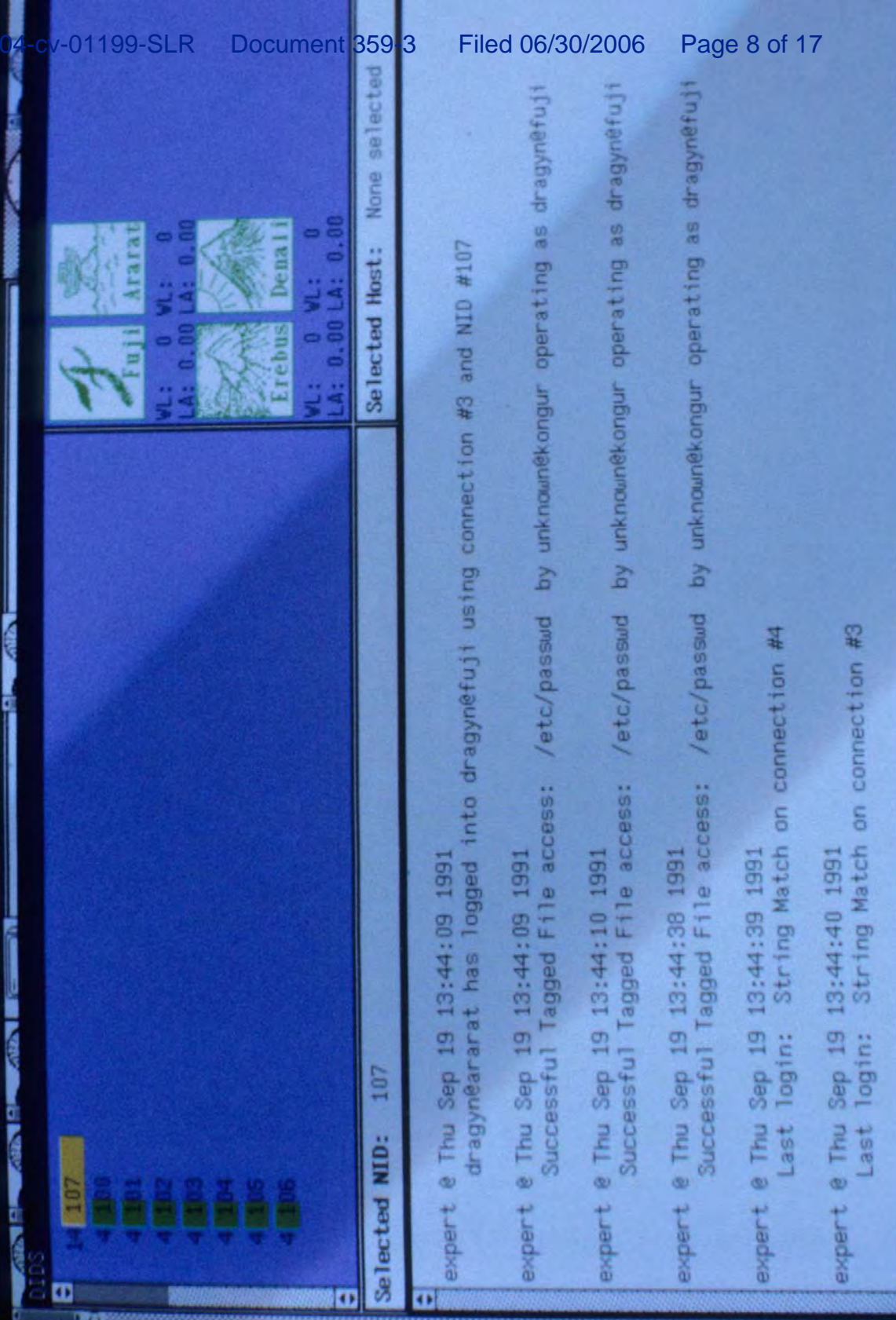
expert @ Thu Sep 19 13:41:52 1991  
Successful Tagged File access: /etc/passwd by unknown@kongur operating as dragyn@ararat

expert @ Thu Sep 19 13:41:53 1991  
Connection #1 has been closed.

update\_hosts\_wl: Host not found  
Tested custom call

HEB\_0004929





HEB\_0004930



LA: 0.00 LA: 0.00

Selected Host: None selected

9 13:44:09 1991

Tagged File access: /etc/passwd by unknown

9 13:44:10 1991

Tagged File access: /etc/passwd by unknown

9 13:44:38 1991

Tagged File access: /etc/passwd by unknown

9 13:44:39 1991

: String Match on connection #4

9 13:44:40 1991

: String Match on connection #3

9 13:44:41 1991

: String Match on connection #2

9 13:44:49 1991

ji has logged into dragynerebus using connect

9 13:44:49 1991

Tagged File access: /etc/passwd by unknown

9 13:44:50 1991

Tagged File access: /etc/passwd by unknown

9 13:47:22 1991

Tagged File access: /etc/passwd by unknown

Host not found  
tem call

Wiretap Direction: ☐ INPUT ☒ OUTPUT

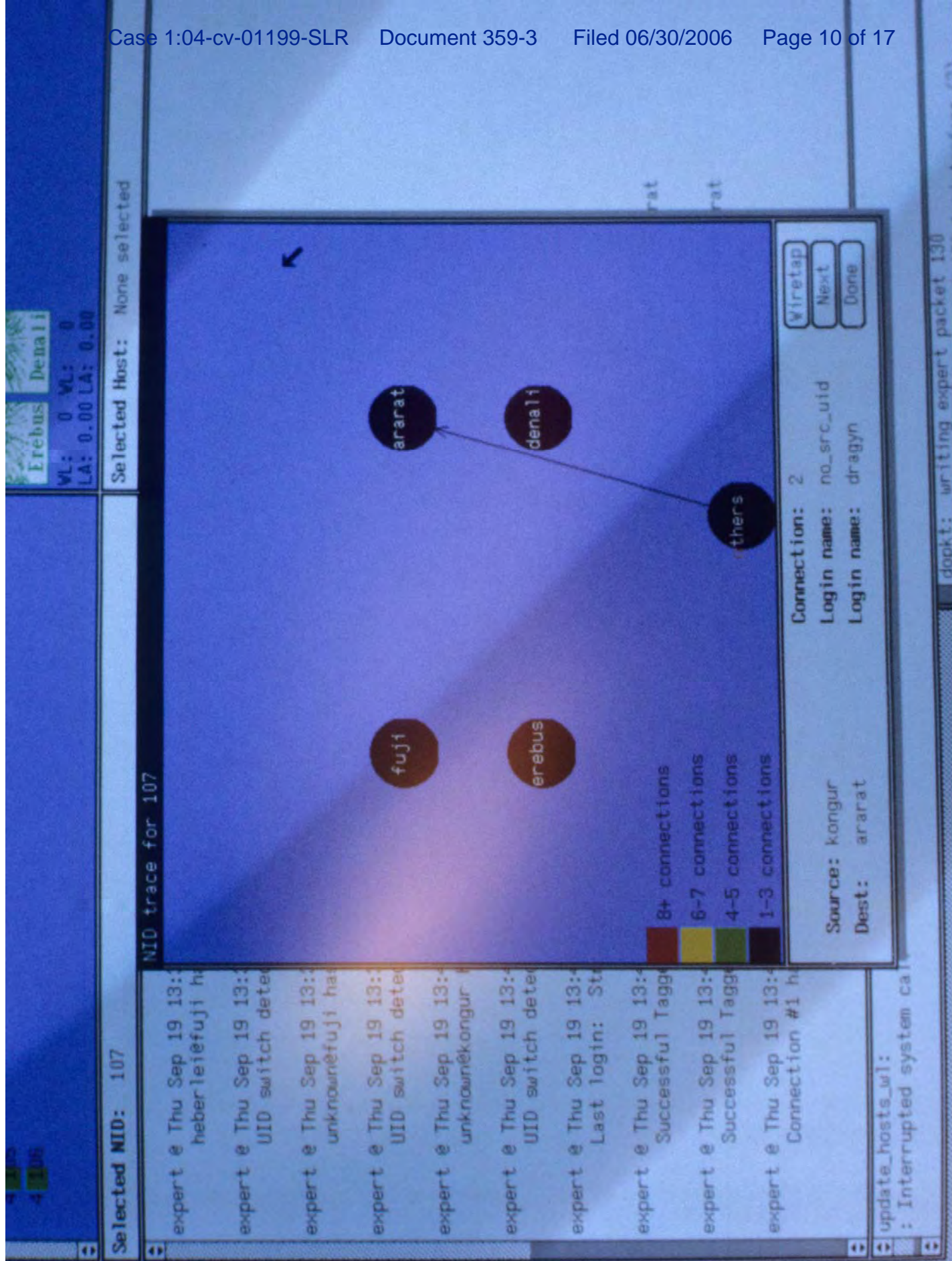
Connection Number: 4

Engage

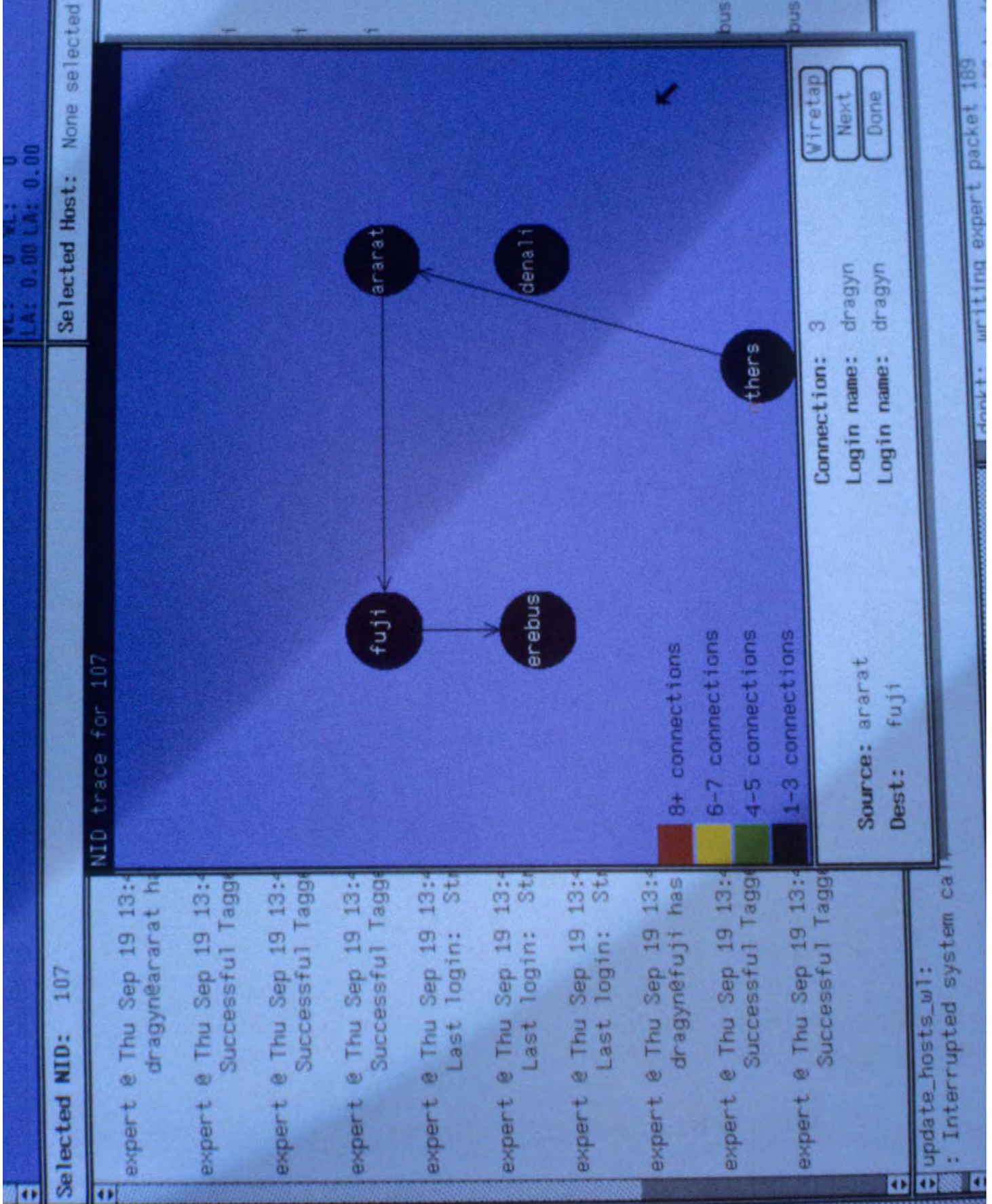
whoami  
dragyn  
erebus% ls  
hello  
erebus%

HEB\_0004931









HEB\_0004933







**NIDS**

15 102  
8 104  
4 100  
4 101  
4 103  
4 105  
4 106

**Selected NID: 107**

**Selected Host: None selected**

expert @ Thu Sep 19 14:02:34 1991  
Last login: String Match on connection #10

expert @ Thu Sep 19 14:02:48 1991  
heberlei@erebus has logged into kongurusing connection #10 and NID #102

expert @ Thu Sep 19 14:02:49 1991  
Multiple NID share same uid. NID #107

expert @ Thu Sep 19 14:02:50 1991  
Multiple NID share same uid. NID #102

expert @ Thu Sep 19 14:02:50 1991  
UID switch detected on NID #102

expert @ Thu Sep 19 14:02:51 1991  
Connection #10 has been closed.

expert @ Thu Sep 19 14:02:59 1991  
Connection #9 has been closed.

expert @ Thu Sep 19 14:03:51 1991  
Successful Tagged File access: /etc/passwd by heberlei@local operating as heberlei@erebus

expert @ Thu Sep 19 14:03:55 1991  
Login incorrect: String Match on connection #8

**Ararat**  
VL: 0 WL: 0  
LA: 0.00 LA: 0.00

**Fuji**  
VL: 0 WL: 0  
LA: 0.00 LA: 0.00

**Erebos**  
VL: 0 WL: 0  
LA: 0.00 LA: 0.00

**Denali**  
VL: 0 WL: 0  
LA: 0.00 LA: 0.00



VL: 0 VL: 0  
LA: 0.00 LA: 0.00

Selected Host: None selected

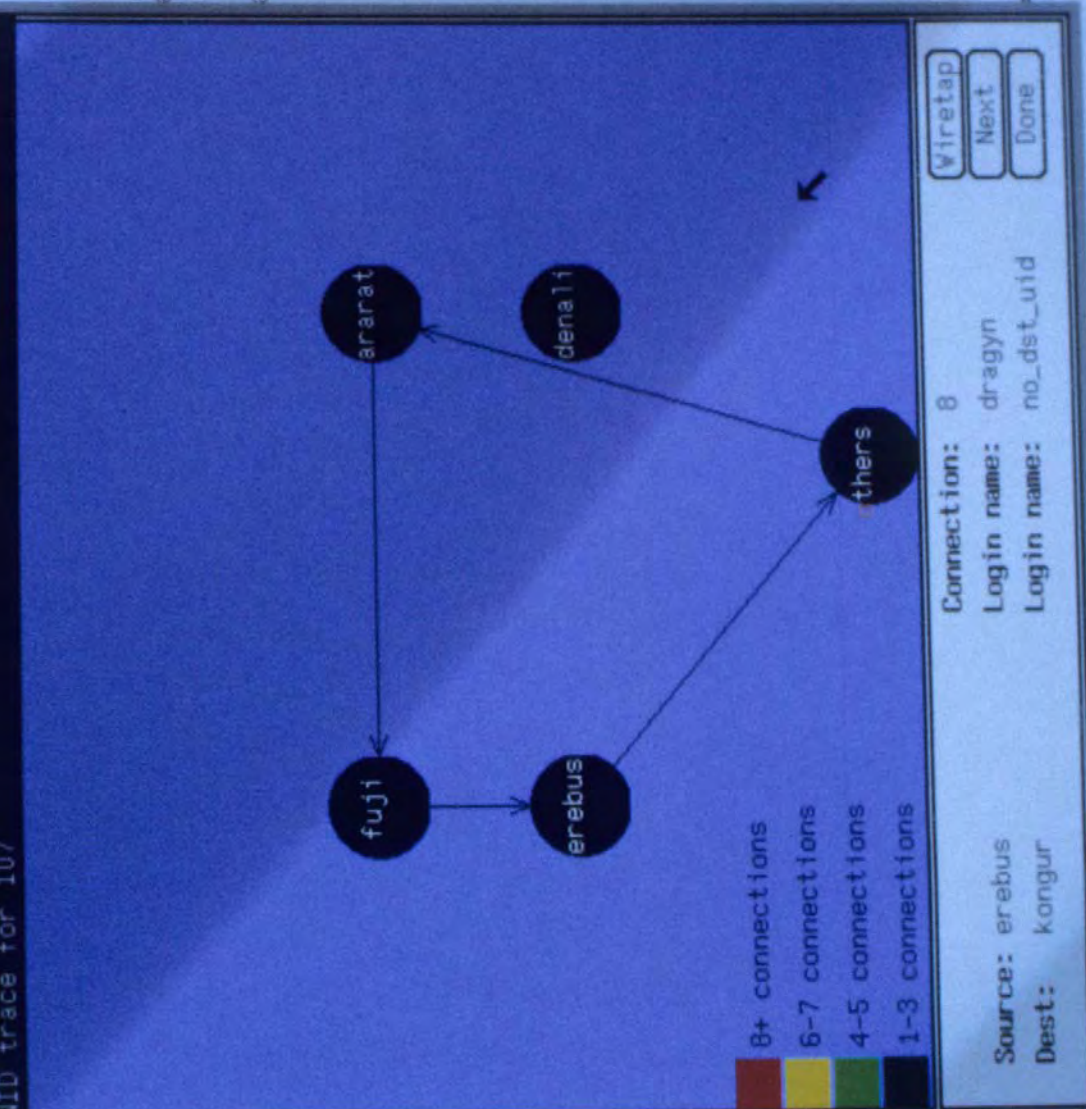
Selected NID: 107

NID trace for 107

expert @ Thu Sep 19 13:5  
xman@erebus has  
expert @ Thu Sep 19 13:5  
Successful Tagg  
expert @ Thu Sep 19 13:5  
Successful Tagg  
expert @ Thu Sep 19 13:5  
Last login: Sta  
expert @ Thu Sep 19 13:5  
Last login: Sta  
expert @ Thu Sep 19 13:5  
Last login: Sta  
expert @ Thu Sep 19 13:5  
Last login: Sta  
expert @ Thu Sep 19 13:5  
dragyn@erebus ha  
expert @ Thu Sep 19 13:5  
Loop detected on  
expert @ Thu Sep 19 13:5  
UID switch deta

update\_hosts\_wl:

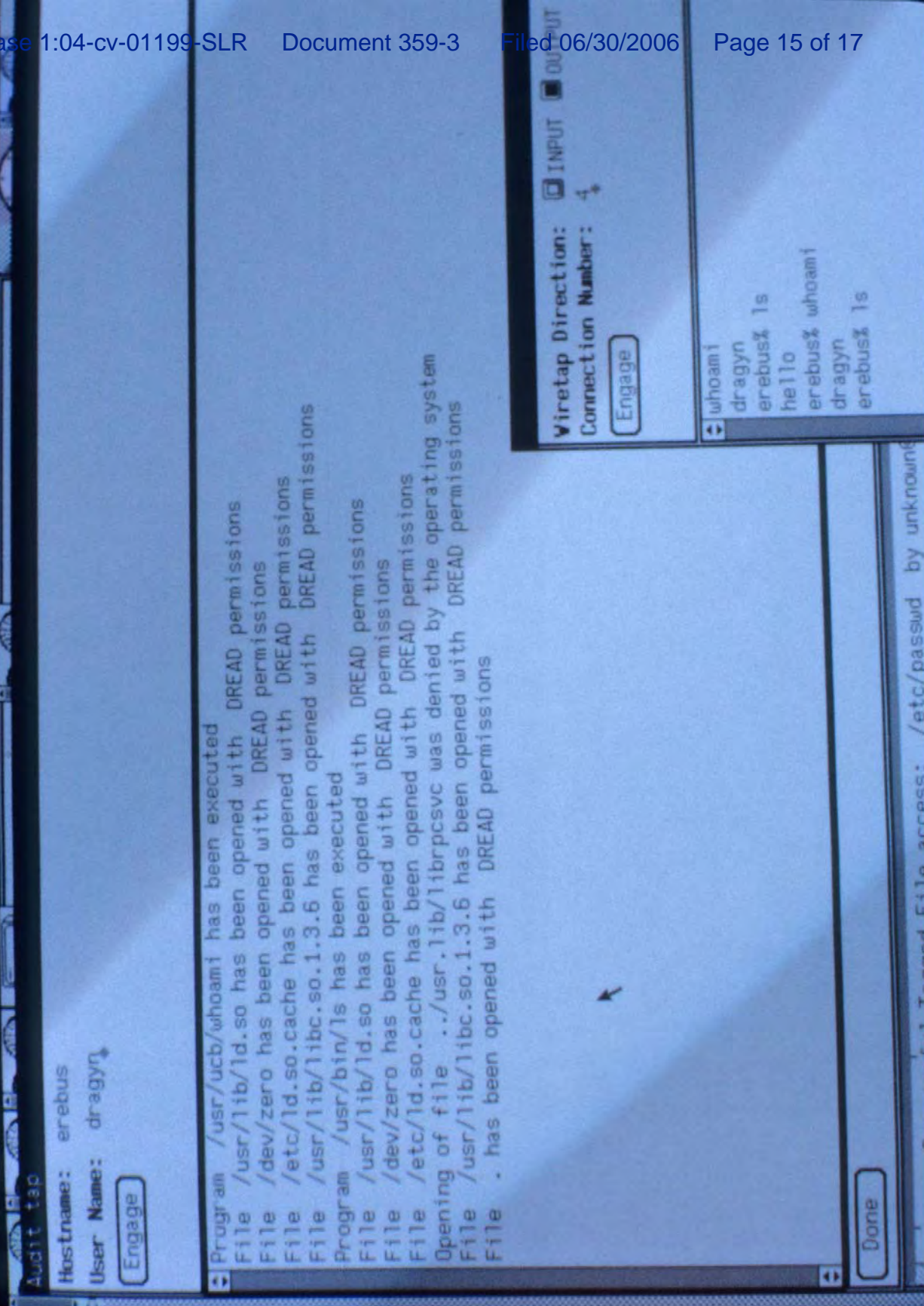
: Interrupted system call



dopkt: writing expert packet 362  
dopkt: sending expert packet 362 to interface (2)

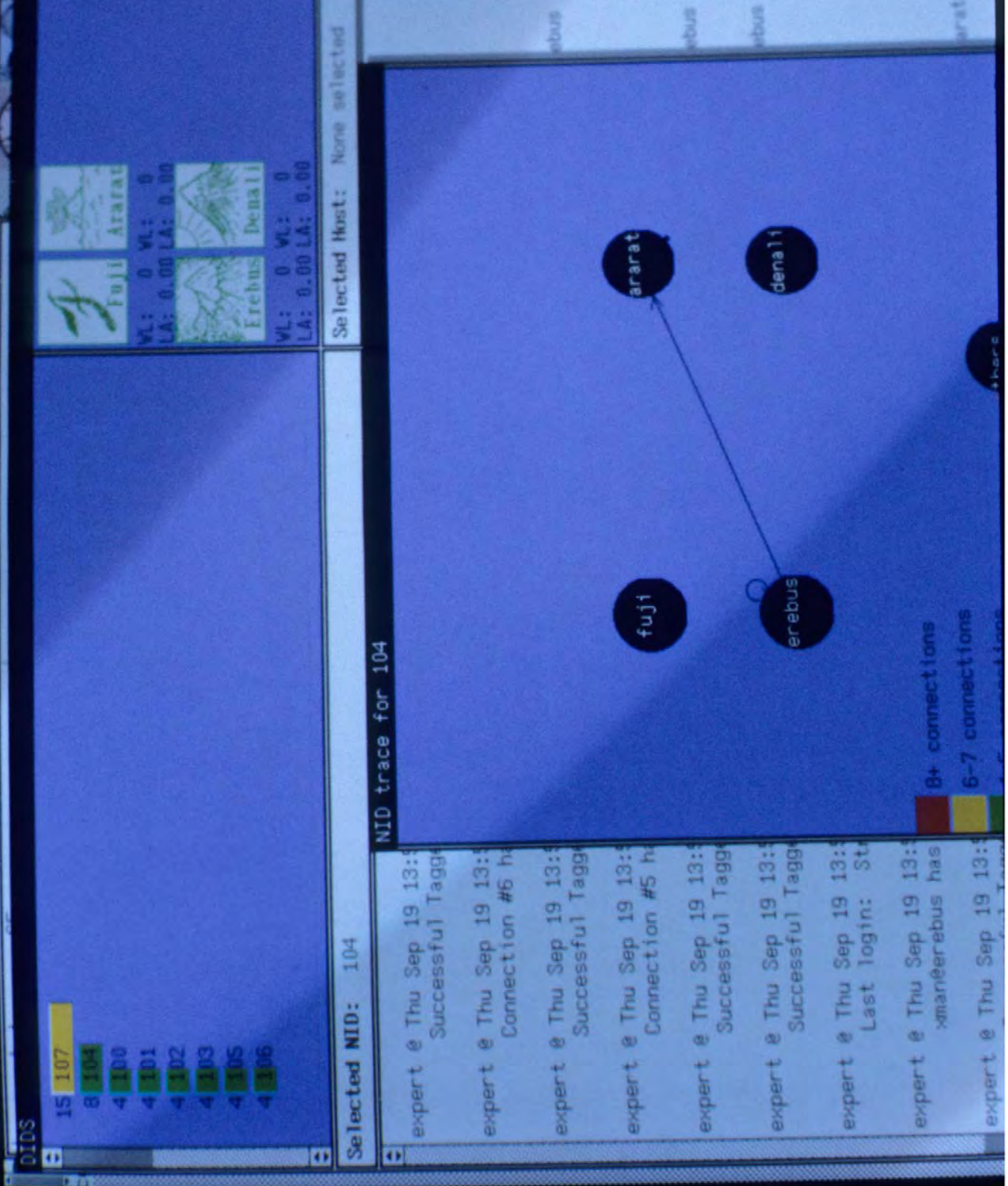
HEB\_0004936





HEB\_0004937









HEB\_0004939